CHAPTER IV

CLOSING

4.1 Conclusion

This study has examined the implementation of e-government in Dramaga Subdistrict with a specific focus on human resource management and its intersection with digital transformation in public service delivery. Drawing upon qualitative analysis and a triangulated approach using field interviews, policy reviews, and theoretical reflection, several key findings have emerged.

At the institutional level, the adoption of digital systems such as SIPD, SiCantik, and electronic correspondence has shown meaningful potential to improve administrative efficiency and transparency. However, these advancements are not evenly distributed across all layers of bureaucracy. As the analysis reveals, the effectiveness of e-government implementation is constrained by generational gaps, unequal digital skills, and organizational inconsistencies in role assignment and system coordination.

From the human resource perspective, the lack of systematic capacity-building, insufficient mentoring schemes, and fragmented recruitment strategies contribute to the stagnation of innovation within the subdistrict government. The mismatch between personnel competencies and digital roles reinforces bottlenecks that inhibit broader digital institutionalization. Informal delegation practices—

though adaptive—are symptomatic of an underlying absence of structured digital governance.

Moreover, when assessed from the perspective of service users, the digital transition has brought both positive outcomes and notable limitations. While some residents benefit from simplified administrative processes and access to information, others—especially elderly or digitally marginalized groups—face barriers in using online services. These gaps affirm the persistence of the digital divide, even as infrastructure expands.

Through the theoretical lens of theory of human capital, public sector innovation, e-government readiness, and the Technology Acceptance Model (TAM), the study underscores that digital transformation in local governance is not solely a technological endeavor, but a multidimensional process shaped by human, institutional, and social dynamics. The success of e-government at the subdistrict level ultimately depends on the alignment between system design, organizational capacity, and citizen readiness.

Despite these insights, several limitations shaped the scope of this study. The research was confined to a single subdistrict, which limits the generalizability of findings across varying administrative settings. Interview access was constrained by time and availability, resulting in a concentration of perspectives from within the local bureaucracy. Quantitative data, such as system usage metrics or longitudinal citizen feedback, were not accessible during the fieldwork, restricting deeper analysis on platform performance. Furthermore, while the study incorporates citizen input, the depth of that perspective remains limited—highlighting the need for future research that gives more space to the voices and experiences of service users.

At the same time, the study challenges the assumption that existing institutional frameworks are sufficient to sustain e-government reforms. Evidence from Dramaga shows that coordination still relies on ad-hoc and informal mechanisms (such as WhatsApp groups), which, while adaptive in the short term, do not guarantee long-term integration or accountability. In practice, this points to institutional fragility rather than strength, suggesting that without formalized processes and structured digital governance, innovation risks being unsustainable.

Finally, the findings raise critical concerns about digital security. Local officials perceive systems as "sufficiently protected as long as the system runs normally," but this reliance on operational stability falls short of best practice. As Al-Khouri (2012) emphasizes, effective governance requires comprehensive data governance frameworks, while ISO/IEC 27001 (Mataracioglu & Ozkan, 2011) stresses ongoing risk assessment, incident response, and access control. For an institution managing sensitive financial and demographic data, the absence of systematic digital security protocols is not merely a technical gap—it is a structural vulnerability that undermines both efficiency gains and public trust.

4.2 Recommendations

While this research illustrates the operational reality of e-government in Dramaga Subdistrict, it also offers strategic entry points for improvement. The findings lead to the following recommendations for local government institutions, stakeholders, and relevant actors:

1. Develop structured and inclusive digital capacity-building programs across all administrative units, with particular attention to senior staff and undertrained personnel, to reduce internal digital gaps.
2. Institutionalize role clarity and competency-based task assignment, ensuring that digital responsibilities are matched with personnel qualifications and supported by formal documentation and evaluation systems.
3. Broaden the role of monitoring and feedback mechanisms by incorporating academic institutions and civil society organizations to assess and co-develop adaptive policies for sustainable e-government governance.
4. Elevate citizen experience as a central metric of success in e-government evaluation frameworks, ensuring that technological advancement translates into meaningful, accessible, and inclusive public service delivery.
5. Formalize a multi-level governance model for e-government, ensuring clear role division between regency-level Diskominfo and subdistrict offices through Regent Decrees or SK, supported by dedicated data stewardship units and standardized coordination mechanisms. This step reduces organizational silos and reinforces accountability in digital governance.

6. Institutionalize an ISO/IEC 27001-aligned Information Security Management System (ISMS), beginning with risk assessment, role-based access control, backup drills, and incident response protocols. Embedding digital security standards provides not only technical safeguards but also institutional legitimacy, ensuring that citizen data is protected within globally recognized frameworks.